Cyber Security Update

Thomas J. Schlagel

Presented to the RHIC-AGS UEC

September 9, 2005

Topics

- Certification and Accreditation
- HSPD-12

What is Certification and Accreditation?

- **Certification** - comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Accreditation** - the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

Certification and Accreditation ensures that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically in accordance with federal or agency policy and whenever there is a significant change to the system or its operational environment.

What are the requirements?

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires that "a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years." and "a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application."

FISMA requires senior agency officials to assess and manage risk to agency IT resources. C&A is the mechanism used to accomplish this function.

DOE Order 205.1 requires Heads of Departmental Elements to "ensure that system Certification and Accreditation (C&A) activities are performed."

Enclaves

DOE Certification and Accreditation is performed at the “enclave” level.

Definition Of Enclave

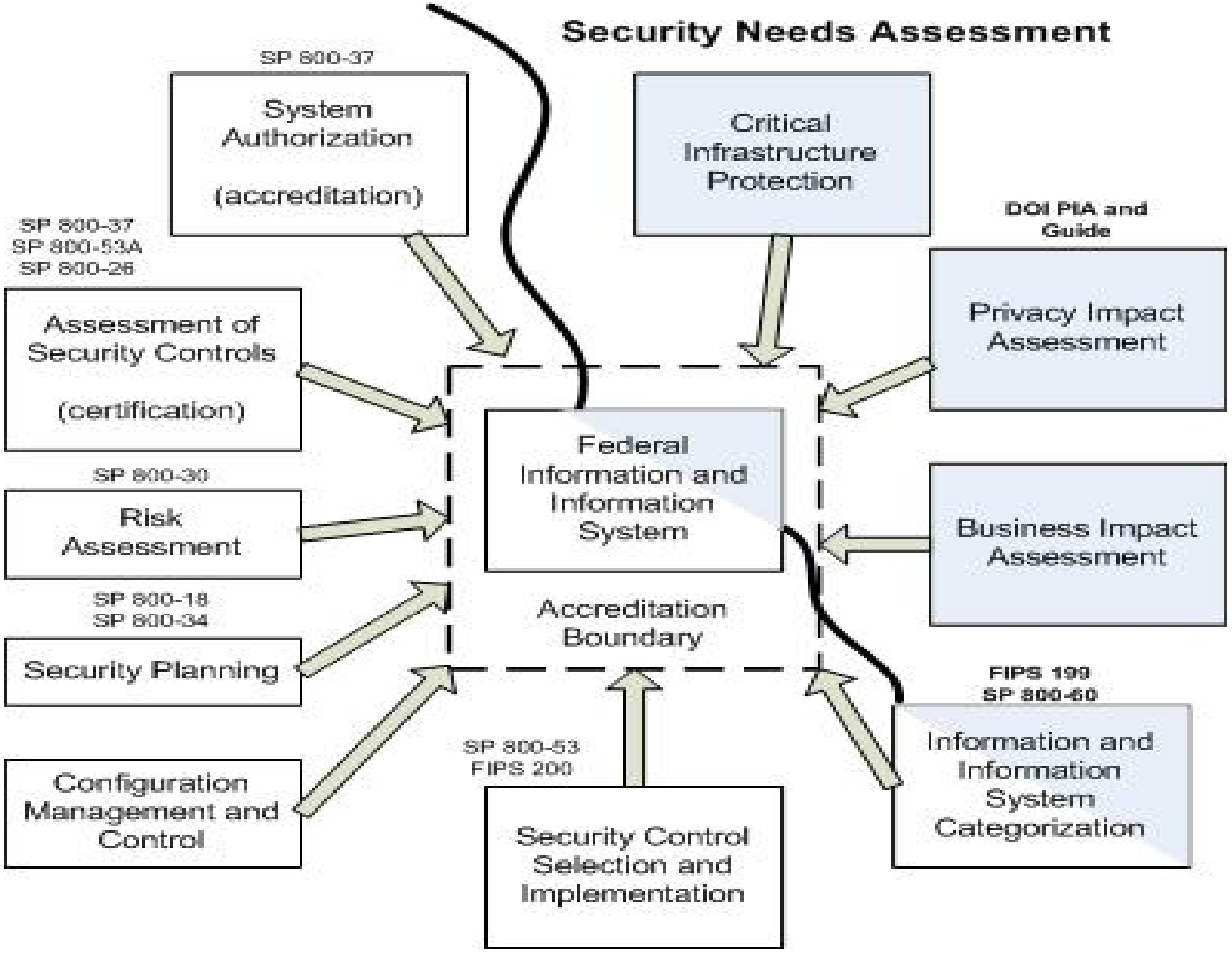
A collection of information and information resources that have similar security protection requirements and are protected as a group. Enclaves include one or more major information systems. An organization may have an enclave or may have several enclaves.

Balance between having too many enclaves (too much documentation) and too few (IS do not share common characteristics)

Common Characteristics Of An Enclave

- Must specify boundaries (all systems within enclave)
- Documentation must reflect composite of controls necessary to safeguard all information contained
- Systems must be under the same management control -- have the same operating characteristics and have the same level of risk of compromise

Aligning Systems With Enclaves



Security Needs Assessment

SP 800-37

System Authorization

(accreditation)

Critical Infrastructure Protection

SP 800-37
SP 800-53A
SP 800-26

Assessment of Security Controls

(certification)

DOI PIA and Guide

Privacy Impact Assessment

Federal Information and Information System

Accreditation Boundary

SP 800-30

Risk Assessment

Business Impact Assessment

SP 800-18
SP 800-34

Security Planning

FIPS 199
SP 800-60

Information and Information System Categorization

Configuration Management and Control

SP 800-53
FIPS 200

Security Control Selection and Implementation

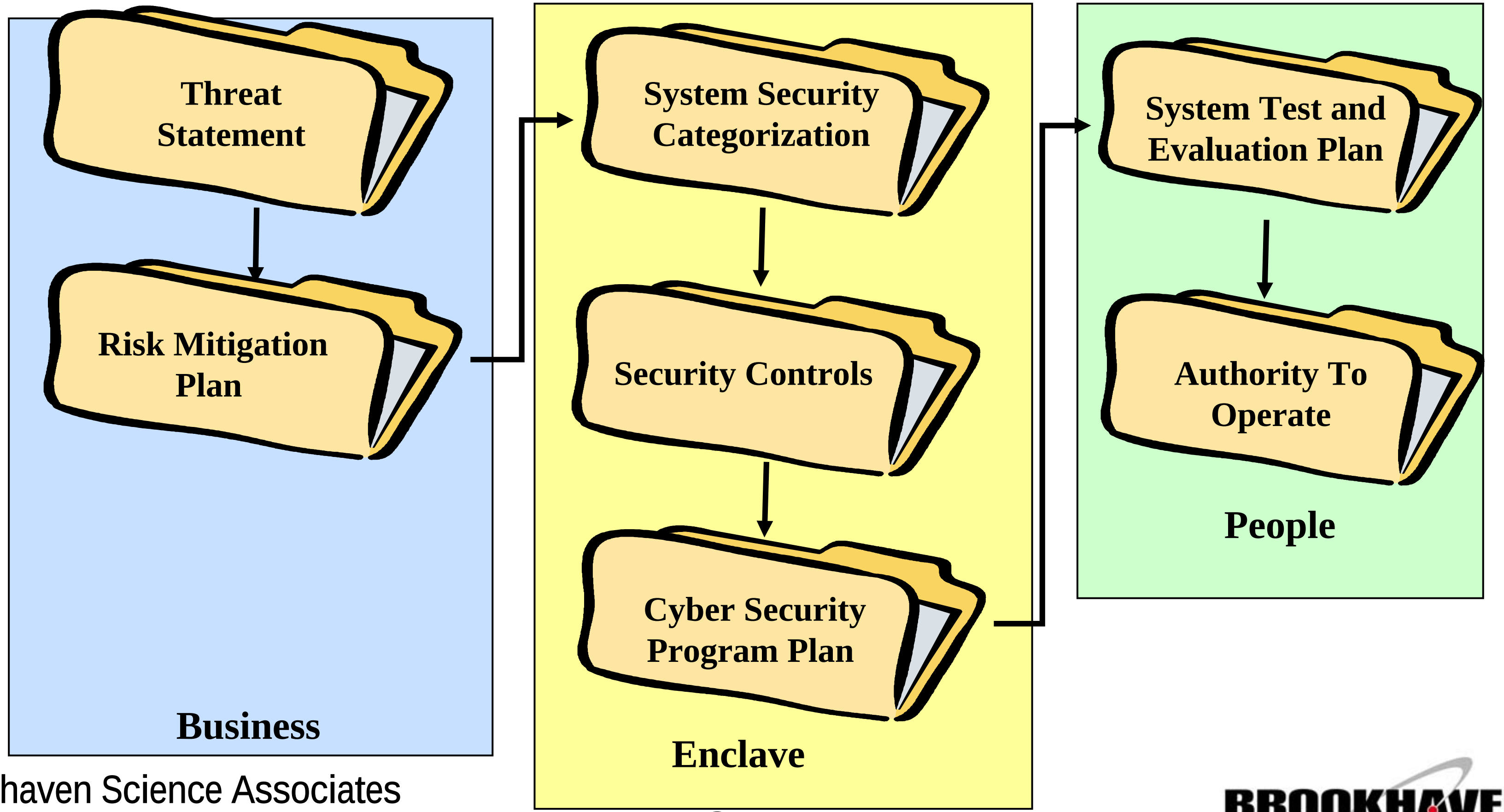
BNL Enclaves

- Research
  - Locally managed systems used primarily for scientific and technical research
  - Mixture of Windows and UNIX/Linux systems
- Administrative
  - Centrally managed systems used primarily for administrative work with standard software
  - No local administrative rights
  - Windows systems
- Business Servers (e.g. PeopleSoft)
- Wireless
- Extranet (e.g. ARM, Visitors network)
  - Completely outside the BNL campus network, but still inside BNL's IP address space

Information systems that cannot fit into one of these categories will need to have additional security controls (e.g. isolated from rest of enclave)

C&A Package

C&A Documentation Package



Threat Statement

Risk Mitigation Plan

Business

System Security Categorization

Security Controls

Cyber Security Program Plan

Enclave

System Test and Evaluation Plan

Authority To Operate

People

C&A Corrective Actions

- C&A Corrective Actions originally scheduled for completion August 30.
- Examination of enclave structure requires restructuring of package – granted 60 day extension to **October 30.**
  - Complete security controls document for Research & Administration enclaves
  - Complete Cyber Security Program Plan (CSPP) for all enclaves
  - Review of all documents
  - Perform gap analysis – from current state to desired state in CSPP – to determine follow on actions
  - BHSO reviews package – accept enclaves, controls, and residual risks (cyber security risks that are not being addressed)
  - BHSO issues Authority to Operate letter
- Great deal of work still remains to complete the package and review before submitting to BHSO.

HSPD-12
Homeland Security Presidential Directive 12

HSPD-12 was issued by the White House on August 27, 2004. Motivated by the need to secure access to Federal and other facilities where there is potential for terrorist attacks, HSPD-12 requires the development and deployment of a common and reliable ID system for Federal employees and contractors that is interoperable across government agencies.

- Requires secure and reliable forms of personal identification:
  - Based on sound criteria to verify an individual employee’s identity
  - Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation
  - Rapid electronic verification of personal identity
  - Identity tokens issued only by providers whose reliability has been established by an official accreditation process
- HSPD-12 Information http://csrc.nist.gov/piv-project

Personal Identity Verification (PIV)

- NIST Computer Security Division was tasked with developing standards, guidelines, recommendations, and/or technical specifications. Federal Information Processing Standard (FIPS) 201 *Personal Identity Verification of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.
- FIPS 201 defines the standards to:
  - protect personal privacy of applicants;
  - authenticate identity source documents;
  - obtain and store biometric data (e.g., fingerprints, facial images);
  - create a "personalized" PIV card with data needed to grant access to Federal facilities and information systems;
  - assure appropriate levels of security for applications; and
  - provide interoperability among Federal organizations

HSPD-12 Implementation Timelines

- PIV-I (Policies and Procedures)
  - Common Identification, Security and Privacy Requirements
    - New personal identity proofing, registration, and issuance process compliant with FIP 201
    - New employees and contractors must go through identity proofing
    - Does **not** require new credential.
  - Completion: **October 27, 2005.**
- PIV-II (Technical Interoperability)
  - Government-wide uniformity and interoperability
    - New PIV credential (smartcard)
    - Required for access to information systems
  - Completion: **October 27, 2006.**
- By **October 27, 2007**, identity proofing should be on record for all current employees and contractors

PIV-I
DOE N206.1 – Identity Proofing

- Draft DOE notice 206.1 issued August 19 (two months before deadline). Describes requirements on identity proofing to be in compliance with FIPS 201.
- Current BNL site credentials can continue to be used during PIV-I even for new employees.
- New identity proofing requirements
  - Fingerprinting
  - Background check (NAC, NACI)
  - Credential can be issued on satisfactory fingerprint + NAC. If NAC results have not returned in 5 days, credential can be issued
- Note – **Foreign Nationals will continue to use the current local site process for the time being**
- Only for new employees/contractors/affiliates. All current credentials for people covered by PIV must be reissued under new process by October 1, 2007.
- Final N 206.1 should be issued next week.

PIV-I Applicability

- Federal employees and contractors. M&O contractors are included.
- Application to affiliates (guests, students, visitors, others) follows 6 month affiliation rule:
    - > 6 months – Long term, needs PIV credential
    - < 6 months – Short term, does not need PIV credential – will need badge that is visually different from current site badge
    - Examples (these are mine, and are still subject to change)
        - NSLS users who use beam line for few days at a time for a few times a year are short term guests – no PIV
        - RHIC experimentalists that are manning detectors are here during the run. If < 6 months, then a short term guest – no PIV
        - Guest researcher that is on site performing work for > 6 months consecutively is a long term guest – requires PIV
        - Based on the final DOE notice, BNL must clearly issue interpretations of long term/short term affiliate
    - There are no clear guidelines for the applicability to guests at this time
- Remote access users
    - These users currently do not need an ID, and are not covered by this notice, but are covered under PIV-II
    - DOE guidance (verbal) is that PIV credential is needed for accessing systems that are Level 2 or greater risk under the OMB e-Authentication criteria. SLCCC interpretation is that majority of SC open lab research systems are Level 1, and therefore should not require a PIV credential. This is an open issue.

PIV-I
Personal Identity Proofing Requirements

Applicant must:

- Appear in person to PIV Registrar with two forms of identification. One must be a state or federal government-issued documents.
- Fill out an OPM Form 85 giving personal information dating back 5 years.
- Have fingerprints taken for background investigation process. Two electronic fingerprints will be used for PIV-II credential.
- Registrar issues a National Agency Check with written Inquiries (NACI) and fingerprint check
- Foreign nationals are not covered by this process. Continue to use current process (IA 473) with fingerprinting.
- A short term badge can be issued while waiting for the results of the background checks, so there should be no disruption in access to the site.
- Credential is issued based on positive background check, or review by adjudication board

PIV-I
Open Issues

- This initiative is still in a state of flux. High levels in DOE are still trying to understand the impacts, so there will likely be more changes.
- Costs for PIV-I are not fully tallied. Additional resources required for credentialing process; background checks; electronic fingerprinting. This is a unfunded mandate.
- Implementation of the directive could have adverse effects to the Science mission. This is still being discussed (Lab Directors meeting)
- Favorable interpretation may remove requirement for PIV-II credential for most remote users
- Adjudication Process – Not clear how this process will work, how negative results will be handled - Waiting for further guidance from DOE.
- Employee communications – putting together Monday Memo article to inform staff, guests about upcoming requirements